Schegge di Cassandra/ OHM2013: SIM ovvero Spie Insicure e Manipolabili

(298) - Attacco alle SIM card dimostrato dall'hacker Karsten Nohl. Che telefona senza SIM per far capire come questo rettangolo di plastica…

Schegge di Cassandra/ OHM2013: SIM ovvero Spie Insicure e Manipolabili

Figure 1:

(298) - Attacco alle SIM card dimostrato dall'hacker Karsten Nohl. Che telefona senza SIM per far capire come questo rettangolo di plastica metta a rischio la rete e i suoi utenti.

29 agosto 2013—Nella precedente Scheggia avevamo riferito ai 24 increduli lettori quello che l'ottimo Philippe Langlois aveva ritenuto di raccontare durante il suo divino seminario di OHM2013.

L'argomento era l'insicurezza di quella parte delle reti cellulari e 3G che forma l'infrastruttura globale (dall'antenna della cella in poi).

Si accennava al fatto che il modello di sicurezza dei vari provider tra loro era di totale trust, cioè che non esisteva alcuna sicurezza.L'infrastruttura di rete non si ferma però all'antenna della cella a cui il vostro cellulare è collegato.

Se fate un attimo mente locale e tornate ai tempi dell'acquisto della vostra prima SIM, ricorderete forse di aver intravisto, tra i pieghevoli consegnativi in quell'occasione, una clausola riguardo al fatto che la SIM è e rimane di proprietà del provider di telefonia mobile, e che dovrebbe addirittura essere restituita al termine del contratto o dietro richiesta del provider stesso.

La SIM nel cellulare quindi non è vostra ma ancora parte dell'infrastruttura di rete cellulare del vostro padrone provider, questione importante visto che la SIM è un oggetto "intelligente", come Cassandra vi aveva già potuto raccontare qualche tempo addietro (grazie alla partecipazione al CCC2011), che è sotto il completo controllo del provider, ed è l'unico punto in cui vengano gestite autenticazione dell'utente e sicurezza complessiva della rete cellulare.

Sintetizzando, si può dire che è l'unico bastione dove viene attuata la difesa della rete dai propri terminali, visti (giustamente) come oggetti potenzialmente malevoli e distruttivi.

Questo significa che nelle reti cellulari non esiste una difesa in profondità, ma solo una difesa perimetrale (e nemmeno completa): basta scavalcare quel punto per trovarsi nella situazione descritta da Philippe.

Ecco un ottimo motivo per alzare il velo del segreto sulla SIM, su questo oggetto intelligente che controlla il vostro dumbphone o smartphone ancor più e ancor prima del suo sistema operativo.

Le specifiche GSM prevedono infatti che il telefonino debba eseguire, senza discussioni e senza avvisare l'utente, qualunque programma venga caricato nella SIM.
Intendiamoci, come nel caso della localizzazione geografica dei cellulari non si tratta di un congegno-spia inserito dall'NSA, ma semplicemente di un modo per gestire la rete cellulare, e ad esempio spiegare al telefono che all'estero è bene che tenti di collegarsi prima ad un provider "amico" (sperabilmente più economico anche per l'utente), piuttosto che a quello indicato dall'utente, o al primo che capita.

Ma potrebbe essere abusato in maniera devastante, proprio come i log di cella che hanno assunto il ruolo di strumenti di tecnocontrollo legalizzato, per fare qualsiasi altra cosa il provider (o chi controlla il provider) ritenga opportuno fare, incluso ad esempio monitorare o disabilitare permanentemente la connessione lato cellulare (non sull'HLR, per intenderci).

Questo sistema di caricamento di software sulla SIM avviene sfruttando particolari "messaggi di controllo", equivalenti ai normali SMS, che trasportano a pezzetti questi software per farli arrivare in automatico ad uno, alcuni o tutti i cellulari collegati ad una rete, dove vengono riassemblati, verificati ed eseguiti.

Ovviamente anche qui sono presenti accorgimenti per evitare che via radio una cella "finta" possa caricare malware ingannando il cellulare. Le SIM moderne (quasi tutte) possiedono al proprio interno una macchina virtuale Java, che certifica e gestisce questi programmi con vari livelli di sicurezza, grazie ad un sistema ben congegnato di chiavi doppie simile a quello dei dispositivi di firma elettronica o dei programmi come GnuPG, PGP e simili.

Sorge spontanea una domanda: è affidabile, o almeno abbastanza affidabile, questo bastione che gestisce contemporaneamente la sicurezza sia della rete cellulare che dei suoi utenti?

Come il noto smanettone Karsten Nohl ci ha dimostrato in diretta nel suo divino seminario "Esercitazione di utilizzo di una scheda SIM" (Hands-on SIM card exploitation) l'equazione "Implementazione proprietaria di Java = sicurezza" è, non troppo sorprendentemente, doppiamente falsa.

Non è questa la sede per approfondire perché il software proprietario sia intrinsecamente meno sicuro di quello aperto, o perché le macchine virtuali Java siano un ottimo posto per cercare e trovare vulnerabilità. Basti dire qui che il il finale del "seminario dimostrativo" è stato registrarsi su una rete cellulare senza usare nessuna SIM.

Anche qui lo ripeto più lentamente ***s-e-n-z-a u-s-a-re n-e-s-s-u-n-a S-I-M***. Alla faccia del modello di sicurezza delle reti cellulari. Karsten lo ha ovviamente fatto con tutte le cautele del caso, utilizzando un provider informato ed un suo numero di telefono, ed ha chiamato solo

un altro suo cellulare facendolo suonare in diretta (e suscitando un'ovazione da stadio); ha però accuratamente evitato di telefonare ad altri numeri o fare operazioni più "potenti", rendendo così (speriamo) inattaccabile dal punto di vista legale la sua dimostrazione.

Nella parte iniziale del seminario Karsten aveva molto opportunamente riassunto il funzionamento a blocchi di una SIM card Java, della sua macchina virtuale, e come fosse possibile sfruttare una vulnerabilità del protocollo di colloquio tra SIM e cellulare per estrarre la chiave privata da una certa marca di SIM molto diffusa ed utilizzarla in un software per pc che facesse finta di essere la SIM stessa.

Ha poi spiegato come questa vulnerabilità fosse stata in precedenza (pochi giorni prima) comunicata al/ai provider interessato/i, insieme ad un ulteriore "hack" utilizzabile per correggere, sempre via SMS di controllo, il baco stesso.

Pare che ben più di 5 milioni di SIM siano state modificate al volo in pochi giorni prima di Blackhat USA 2013 ed OHM2013.

Con l'augurio che video e slide vengano presto pubblicati anche su sito di OHM, potete nel frattempo deliziarvi con le equivalenti di Blackhat 2013 qui.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on March 20, 2023.

Canonical link

Exported from Medium on August 27, 2025.